Docket No. 200701958-2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:	
Iyad Qumei	
Serial No. 10/813,212	
Filed: March 30, 2004	
For: Electronic Device Network Supporting Enciphering And Deciphering And Update Generation In Electronic Devices	**Electronically filed on April 3, 2008.**
Examiner: Chen, Shin Hon	
Group Art Unit: 2131	
Confirmation No. 4068	

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The Applicant respectfully requests that the Board of Patent Appeals and Interferences reverse the final rejection of claims 1-41 of the present application. This Appeal Brief is timely because it is being filed within one month of the March 6, 2008 mailing date of the Notice of Panel Decision from Pre Appeal Brief Review.

REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

The real party in interest is Hewlett-Packard Development Company, L.P., having a place of business in Houston, Texas.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

Not applicable.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

The present application includes claims 1-41, all of which remain rejected.[1] The Applicant identifies claims 1-41 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

Subsequent to the final rejection of claims 1-41 mailed November 23, 2007, the Applicant filed a Notice of Appeal and Pre Appeal Brief Request for Review on January 17, 2008. The Applicant did not amend any of the claims after the final Office Action was mailed.

[1] *See* November 23, 2007 Final Office Action and March 6, 2008 Notice of Panel Decision from Pre-Appeal Brief Review.

SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

Independent claim 1 recites the following:

An electronic device network for updating at least one of firmware and software in a plurality of electronic devices using at least one electronic device update,[2] the network comprising:

at least one update generator adapted to generate updates,[3] the at least one update generator comprising an encrypting and decrypting engine;[4]

at least one update store storing a plurality of electronic device updates;[5]

at least one update delivery server adapted to dispense the plurality of electronic device updates;[6] and

wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted.[7]

---

[2] *See* present application at, *e.g.,* page 3, lines 2-4, page 12, lines 13-15, Figure 2, ref. 205.
[3] *See id., e.g.,* at page 3, lines 6-7, page 12, lines 20-22, Figure 2, ref. 255.
[4] *See id., e.g.,* at page 3, lines 7-8, page 12, lines 22-24, Figure 2, ref. 257.
[5] *See id., e.g.,* at page 3, lines 8-9, page 12, lines 24-25, Figure 2, ref. 253.
[6] *See id., e.g.,* at page 3, lines 9-10, page 12, lines 27-29, Figure 2, ref. 245.
[7] *See id., e.g.,* at page 3, lines 4-6 and page 11, lines 25-26, page 12, lines 16-19, page 13, lines 2-5, page 13, lines 23-25.

Independent claim 13 recites the following:

A method of updating encrypted information within a firmware image in electronic devices,[8] the method comprising:

generating binary difference information using a first firmware image and a second firmware image,[9] wherein one or both of the first and second firmware images are partially or entirely encrypted,[10] and wherein generating comprises decrypting encrypted portions of the first and second firmware images;[11]

creating an encrypted update for an electronic device using the binary differencing information;[12] and

encrypting firmware images by applying at least one of stream symmetric enciphering and block symmetric enciphering.[13]

Independent claim 22 recites the following:

An electronic device employing one of encrypting and decrypting techniques to update firmware and software,[14] the electronic device comprising:

random access memory;[15] and

non-volatile memory,[16] the non-volatile memory comprising:

---

[8] *See id., e.g.,* at page 5, lines 1-2, page 11, lines 1-3.
[9] *See id., e.g.,* at page 14, lines 8-11 and 16-21, page 17, lines 20-25, Figure 4, refs. 460 and 470.
[10] *See id., e.g.,* at page 17, lines 10-12, page 14, lines 3-7.
[11] *See id., e.g.,* at page 17, lines 13-16, page 14, lines 8-11.
[12] *See id., e.g.,* at page 5, lines 2-4, page 5, lines 14-15, page 14, lines 17-19.
[13] *See id., e.g.,* at page 5, lines 4-5, page 14, lines 24-29.
[14] *See id., e.g.,* at page 6, lines 5-6, page 12, lines 1-4, Figure 1, ref. 105.
[15] *See id., e.g.,* at page 6, line 7, page 12, lines 5-6, Figure 1, ref. 125.
[16] *See id., e.g.,* at page 6, line 7, page 12, lines 5-6, Figure 1, ref. 111.

an update agent;[17]

a first in first out (FIFO) memory device;[18]

a firmware;[19]

a software application;[20] and

an update,[21] wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating,[22] and wherein updating at least one of the firmware and the software application comprises decrypting the encrypted portion.[23]

Independent claim 31 recites the following:

A method of building a firmware upgrade for use in an electronic device incorporating encryption,[24] the method comprising:

building a firmware image to be encrypted,[25] the firmware image comprising a plurality of components;[26] and

encrypting the components before assembling the components into an encrypted firmware image.[27]

---

[17] *See id., e.g.,* at page 6, line 8, page 12, line 8, Figure 1, ref. 127.
[18] *See id., e.g.,* at page 6, lines 8-9, page 12, lines 8-9, Figure 1, ref. 113.
[19] *See id., e.g.,* at page 6, lines 8-9, page 12, lines 8-9, Figure 1, ref. 117.
[20] *See id., e.g.,* at page 6, lines 8-9, page 12, lines 8-10, Figure 1, ref. 121.
[21] *See id., e.g.,* at page 6, lines 8-9, page 12, lines 8-10, Figure 1, ref. 115.
[22] *See id., e.g.,* at page 3, lines 4-6, page 6, lines 9-11 and 12-14. page 7, lines 6-10.
[23] *See id., e.g.,* at page 3, lines 7-8, page 13, line 26 to page 14, line 2.
[24] *See id., e.g.,* at page 7, lines 15-16, page 17, line 17 to page 18, line 26.
[25] *See id., e.g.,* at page 7, lines 16-17, page 17, lines 3-4, Figure 3, ref. 350.
[26] *See id., e.g.,* at page 7, lines 17-18, page 17, lines 3-7, Figure 3, refs. 330, 331, 332,

Dependent claim 36 recites the following:

The method according to claim 35, wherein during at least one of the pre-check analysis and the check recovery analysis, a cyclic redundancy check of a firmware image block is compared against an original image cyclic redundancy check stored in a data update package, wherein when ciphered data is present, the pre-check analysis is performed upon the block to be decrypted before the cyclic redundancy check is calculated.[28]

Dependent claim 37 recites the following:

37. The method according to claim 36, wherein cyclic redundancy check values for ciphered data are stored in the data update package.[29]

Dependent claim 40 recites the following:

40. The method according to claim 39, further comprising a fault tolerant upgrade, the fault tolerant upgrade[30] at least comprising:

maintaining each original data block intact until the original data block is overwritten by an encrypted updated data block;[31] and

maintaining a data update package intact throughout the fault tolerant upgrade.[32]

---

333 and 334.
[27] *See id., e.g.,* at page 7, lines 18-19, page 17, lines 7-8, Figure 3, ref. 360.
[28] *See id., e.g.,* at page 8, lines 8-13.
[29] *See id., e.g.,* at page 8, lines 14-15.
[30] *See id., e.g.,* at page 8, line 27 to page 9, line 2.
[31] *See id., e.g.,* at page 8, line 27 to page 9, line 2.
[32] *See id., e.g.,* at page 8, line 27 to page 9, line 2.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
(37 C.F.R. § 41.37(c)(1)(vi))

- Claims 1-9 and 12 stand rejected under 35 U.S.C. § 102(a) as being anticipated by United States Patent Application Publication No. 2003/0051160 ("Selkirk").
- Claims 10, 11 and 13-41 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Selkirk in view of United States Patent No. 6,230,316 ("Nachenberg").

ARGUMENT
(37 C.F.R. § 41.37(c)(1)(vii))

The Examiner has maintained the rejections of claims 1-41. As shown above, Selkirk forms the basis for all the claim rejections.

Claims 1-12 should be in condition for allowance at least because neither of the cited references describes, teaches or suggests "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted," or "at least one update generator adapted to generated updates, the at least one update generator comprising and encrypting and decrypting engine," as recited in claim 1.

Claims 13-21 should be in condition for allowance at least because neither Selkirk, nor Nachenberg describes, teaches or suggests "generating binary difference information using a first firmware image and a second firmware image, wherein one or both of the first and second firmware images are partially or entirely encrypted, and wherein generating comprises decrypting encrypted portions of the first and second firmware images," as recited in claim 13.

Claims 22-30 should be in condition for allowance at least because the cited references, alone or in combination with one another, do not describe, teach or suggest an electronic device employing one of encrypting and decrypting techniques to update firmware and software, as recited in claim 22.

Claims 31-41 should be in condition for allowance at least because neither of the cited references describes, teaches or suggests anything relating to components of a firmware image of an electronic device, assembling such components into a firmware image of an electronic device, or "encrypting the components before assembling the components into an encrypted firmware image," as recited in claim 31.

I. Selkirk Does Not Anticipate Claims 1-9 And 12

The Applicant first turns to the rejection of claims 1-9 and 12 as being anticipated by Selkirk. "A claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in **a single prior art reference**." *Verdegaal Bros. v. Union Oil Co. of Califomia,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (emphasis added). "The **identical** invention must be shown in as complete detail as is contained in ... the claim." *Richardson v. Suzuki Motor Co.,* 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

Claim 1 recites "an electronic device network for updating at least one of firmware and software in a plurality of electronic devices using at least one electronic device update, the network comprising at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and

decrypting engine; at least one update store storing a plurality of electronic device updates; at least one update delivery server adapted to dispense the plurality of electronic device updates; and **wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted**." As detailed below, the Applicant respectfully submits that Selkirk fails to describe, teach or suggest at least "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices, is encrypted."

Instead of encrypting at least a portion of firmware and/or software in a plurality of electronic devices, Selkirk discloses a "method, computer program product, and firmware device for directly downloading data from a server in a network to a firmware device, bypassing any unencrypted transmission through computer system with which the firmware device may be associated, so that copies of the data are not as readily made...." *See* Selkirk at Abstract.

The Office action asserts that Selkirk discloses "...an electronic device network for updating at least one of firmware and software in a plurality of electronic devices using at least one electronic device update ... wherein at least one of the firmware and software in the plurality of electronic devices and the at least one update being encrypted (Selkirk: [0009] and [0017])...." *See* November 23, 2007 Office Action at page 2. Indeed, the Office Action cites Selkirk **only** at [0009] and [0017] in the rejection of claim 1. Thus, the Applicant will address each of these cited paragraphs:

First, Selkirk discloses the following:

> Accordingly, the present invention is directed towards a method, computer program product, and firmware device for downloading data from a server in a network to a firmware device, bypassing any unencrypted transmission through computer system with which the firmware device may be associated, so that copies of the data are not as readily made. A computer sends a request to a server to download the particular data to a particular firmware device. The server contacts the firmware device directly through the network to initiate the transfer. The server and firmware device communicate over an encrypted data channel so as to prevent any third party, including the aforementioned computer, from intercepting and storing the transmitted data.

Id. at [0009]. This passage of Selkirk merely tracks the language of the Abstract of Selkirk, which the Applicant addressed above. This cited portion and the Abstract of Selkirk do not describe, teach or suggest "...wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted...", as recited in claim 1. In fact, Selkirk fails to describe, teach or suggest anything regarding **updating encrypted firmware or software**. Instead, the Applicant respectfully submits that Selkirk discloses "...a firmware device, data processing system, method, and computer program product for downloading data from a network while preventing piracy of copyrighted material once downloaded" (*id.* at [0002]), which differs from "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted," as recited in claim 1.

Moving on, Selkirk also discloses the following:

> FIG. 1 depicts a distributed data processing system 100 in which the processes of the present invention may be implemented. Computer 102 connects to Internet 104, through which computer 102 communicates with server 106

> and firmware device 108, which is located within computer 102 (although it could be located within a different computer, in an alternative embodiment). **In an embodiment of the present invention, computer 102 requests from server 106 that an update to computer 102's firmware be downloaded from server 106 to firmware device 108.** Firmware device 108, stores code and data that defines the fundamental functionality of a hardware device, for use by computer 102 or one or more peripheral devices in association with computer 102. Firmware device 108 may be, for instance, a monolithic integrated circuit, but it may comprise any combination of hardware components, including discrete logic circuitry, multiple integrated circuits, optical storage, and any other suitable storage medium. **In fulfillment of the request, server 106 contacts firmware device 108 via relay through computer 102 and sends the data over an encrypted communications channel to the firmware device 108, where the data is decrypted.** No decryption of the data takes place outside of firmware device 108. Thus, no unauthorized copies of the data can be made, since only firmware device 108 can decrypt the encrypted transmission. In a preferred embodiment, the encrypted communications channel is established by means of the Secure Sockets Layer (SSL) protocol, described in more detail in FIG. 3, although any one of a number of different encryption schemes and protocols could be used.

Id. at [0017] (emphasis added). The Applicant respectfully submits that there simply is nothing in the portion of Selkirk reproduced above and specifically cited by the Office action that describes, teaches or suggest "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted," as recited in claim 1.

Additionally, the Applicant respectfully submits that Selkirk fails to describe, teach or suggest "at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine," as recited in claim

1. As noted above, the Office action merely discloses Selkirk at [0009] and [0017] as disclosing the various limitations of claim 1. *See* November 23, 2007 Office Action at page 2. As shown above, Selkirk at [0009] does not describe the relevant limitations.

Further, Selkirk at [0017] fails to mention anything about **generating an update**. Indeed, the Applicant respectfully submits that Selkirk taken in its entirety **does not describe, teach or suggest generating an update.** Instead, the portion of Selkirk that the Office Action relies on states that "...[i]n an embodiment of the present invention, computer 102 requests from server 106 that an update to computer 102's firmware be downloaded from server 106 to firmware device 108." Selkirk provides no details how the update came to exist, or how the server 106 came into possession of the update, and certainly fails to teach or suggest that the server 106 generated the update. Instead, Selkirk simply states that "...[i]n fulfillment of the request, server 106 contacts firmware device 108 via relay through computer 102 and sends the data over an encrypted communications channel to the firmware device 108, where the data is decrypted."

The Applicant respectfully submits that the teachings of Selkirk related to encryption and the updating of firmware and software are primarily concerned with the transmission of an update using an encrypted transmission means from server 106 to the firmware device 108. The Applicant respectfully submits that Selkirk fails to teach or suggest "at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine" or "wherein at least

a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted...," as recited in claim 1 of the present application.

The Office Action responds to the Applicant by stating the following:

> Regarding applicant's remarks, applicant argues that the prior art of record does not disclose "at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted". However, Selkirk discloses that the firmware updates are provided to the firmware through secure communication such as SSL, which is encrypted communication (Selkirk: [0017] lines 18-21: send encrypted data to the firmware device).

November 23, 2007 Office Action at page 8. Thus, the Office Action specifically relies on Selkirk at [0017], lines 18-21 as disclosing "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted," as recited in claim 1.

This portion of Selkirk, which the Office Action specifically relies on, discloses, however, the following:

> In fulfillment of the request, server 106 contacts firmware device 108 via relay through computer 102 and sends the data **over an encrypted communications channel to the firmware device 108,** where the data is decrypted.

Selkirk at [0017], lines 18-22 (emphasis added). Notably, this specific portion of Selkirk merely discloses that data is sent over an encrypted channel **to** a firmware device, where the data is decrypted. Thus, the **data** is sent over an encrypted channel and the **data** is decrypted. Neither this portion, nor the remainder, of Selkirk describes, teaches or suggests that any portion of the firmware itself is decrypted. Instead, this portion

merely states that the data is decrypted (and sent to firmware over a decrypted channel). That is, Selkirk does not describe, teach or suggest "wherein at least a portion **of the at least one of firmware and software** in the plurality of electronic devices **is encrypted**," as recited in claim 1. Because the Office Action has not provided any reference that describes, teaches or suggests such a limitation, the Office Action has failed to establish a *prima facie* case of anticipation with respect to claims 1-9 and 12.

Next, the Office Action responds to the Applicant by stating that "Selkirk discloses the server generates firmware updates and transmit the updates to the firmware through secure communication (Selkirk: [0017] lines 8-10: the server generates and provides the updates to firmware)." *See* November 23, 2007 Office Action at page 8. As shown, the Office Action specifically cites Selkirk at [0017], lines 8-10 as disclosing "at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine," as recited in claim 1.

This specific cited portion of Selkirk discloses, however, the following:

> In an embodiment of the present invention, computer 102 requests from server 106 that an update to computer 102's firmware be downloaded from server 106 to firmware device 108.

See Selkirk at [0017], lines 7-10. Notably, this passage of Selkirk, which the Office Action specifically relies on, states that an update to firmware may be downloaded. As discussed above, Selkirk provides no details as to how the update came to exist, or how

the server 106 came into possession of the update, and certainly fails to describe, teach or suggest that the server 106 generated the update. Thus, the Applicant respectfully maintains that Selkirk does not describe, teach or suggest "at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine," as recited in claim 1. Because the Office Action has not provided any reference that describes, teaches or suggests such a limitation, the Office Action has failed to establish a *prima facie* case of anticipation with respect to claims 1-9 and 12.

For at least the reasons discussed above, the Applicant respectfully submits that the Office action has failed to show where Selkirk describes, teaches or suggests each and every element of claim 1, as required by M.P.E.P. §2131. Thus, the Office has failed to establish a *prima facie* case of anticipation with respect to claims 1-9 and 12. Therefore, the Applicant respectfully requests that this rejection be reversed.

II. The Proposed Combination Of Selkirk And Nachenberg Does Not Render Claims 10, 11 and 13-41 Unpatentable

The Applicant now turns to the rejection of claims 10, 11 and 13-41 as being unpatentable over Selkirk in view of Nachenberg.

> The legal concept of *prima facie* obviousness is a procedural tool of examination which applies broadly to all arts. It allocates who has the burden of going forward with production of evidence in each step of the examination process.
>
> * * *
>
> The examiner bears the initial burden of factually supporting

> any *prima facie* conclusion of obviousness. **If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.**

See M.P.E.P. at § 2142 (emphasis added).

Initially, the Applicant respectfully submits that the proposed combination does not render claims 10 and 11 unpatentable for at least the reasons discussed above with respect to claim 1.

A. The Proposed Combination Does Not Render Claims 13-21 Unpatentable

The Applicant respectfully submits that the proposed combination of Selkirk and Nachenberg fails to describe, teach or suggest, for example, a method of updating encrypted information within a firmware image in electronic devices, the method comprising generating binary difference information using a first firmware image and a second firmware image, wherein one or both of the first and second firmware images are partially or entirely encrypted, and wherein generating comprises decrypting encrypted portions of the first and second firmware images; creating an encrypted update for an electronic device using the binary differencing information; and encrypting firmware images by applying at least one of stream symmetric enciphering and block symmetric enciphering, as recited in independent claim 13.

More specifically, the Applicant respectfully submits that the proposed combination of references fails to teach or suggest, at least "generating binary difference information using a first firmware image and a second firmware image,

wherein one or both of the first and second firmware images are partially or entirely encrypted, and wherein generating comprises decrypting encrypted portions of the first and second firmware images," for at least the reasons discussed above. Neither Selkirk nor Nachenberg make any mention of **generating binary difference information using firmware images that are partially or entirely encrypted**. The cited references also necessarily fail to describe, teach or suggest that the generating comprises decrypting encrypted portions of the firmware images. .

For at least the reasons discussed above, the Applicant respectfully submits that the proposed combination of Selkirk and Nachenberg fails to describe, teach or suggest all of the limitations of claim 13. Thus, the Office action has failed to establish a *prima facie* case of obviousness with respect to claims 13-21.

B. The Proposed Combination Does Not Render Claims 22-30 Unpatentable

The Applicant respectfully submits that Selkirk and Nachenberg, alone or in combination, do not teach, suggest, or disclose, for example, an electronic device employing one of encrypting and decrypting techniques to update firmware and software, the electronic device comprising random access memory; and non-volatile memory, the non-volatile memory comprising an update agent; a first in first out (FIFO) memory device; a firmware; a software application; and an update, wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating, and wherein updating at least one of the firmware and the software application comprises decrypting the

encrypted portion. Indeed, the Office Action has not attempted to show or explain where the cited references describe the limitations noted above. *See* November 23, 2007 Office Action at page 8. In particular, the Office action summarily states that "claims 22-41 are rejected based on the same reasons set forth above in rejecting claims 1-21," but offers no evidence or citations from the references as support. *See* November 23, 2007 Office Action at page 8. Thus, for at least this reason, the Office Action has wholly failed to establish a *prima facie* case of obviousness with respect to these claims.

Additionally, the Applicant respectfully submits that the proposed combination of references fails to describe, teach or suggest at least, "...non-volatile memory comprising ... a first in first out (FIFO) memory device," as recited in claim 22. **Both Selkirk and Nachenberg are silent in this regard, and provide no teachings related to such a device.**

For at least the reasons discussed above, the Applicant respectfully submits that the proposed combination of Selkirk and Nachenberg fails to describe, teach or suggest all of the limitations of claim 22. Thus the Office action has failed to establish a *prima facie* case of obviousness with respect to claims 22-30.

C. The Proposed Combination Does Not Render Claims 31-41 Unpatentable

With regard to claim 31, the Applicant respectfully submits that Selkirk and

Nachenberg, alone or in combination, do not describe, teach, or suggest, for example, a method of building a firmware upgrade for use in an electronic device incorporating encryption, the method comprising building a firmware image to be encrypted, the firmware image comprising a plurality of components; and encrypting the components before assembling the components into an encrypted firmware image. Indeed, the Office Action does not even attempt to show where such limitations are found in the cited references. *See* November 23, 2007 Office Action at page 8 ("As per claims 22-41, claims 22-41 encompass the same scope and obvious variation of claims 1-21. Therefore, claims 22-41 are rejected based on the same reasons set forth above in rejecting claims 1-21."). A review of claims 22-41 demonstrates, however, that they are not the same as claims 1-21. As such, they cannot be rejected merely by stating that the same rejections as those set forth with respect to claims 1-21 are equally applicable. For at least this reason, the Office Action has failed to establish a *prima facie* case of obviousness with respect to claims 31-41.

Further, the Applicant respectfully submits that neither Selkirk nor Nachenberg describes, teaches or suggests anything with respect to components of a firmware image of an electronic device, of assembling such components into a firmware image of an electronic device. Also, the cited references fail to describe, teach or suggest anything with respect to "encrypting the components before assembling the components into an encrypted firmware image," as recited in claim 31.

For at least these reasons, the Applicant respectfully submits that the Office

action has failed to establish a *prima facie* case of obviousness with respect to claims 31-41.

D. The Proposed Combination Does Not Render Claim 36 Unpatentable

Claim 36 recites, in part, "wherein during at least one of the pre-check analysis and the check recovery analysis, a cyclic redundancy check of a firmware image block is compared against an original image cyclic redundancy check stored in a data update package, wherein when ciphered data is present, the pre-check analysis is performed upon the block to be decrypted before the cyclic redundancy check is calculated." The Applicant respectfully submits that Selkirk and Nachenberg are devoid of anything that describes, teaches or suggests a "cyclic redundancy check." Thus, for at least this additional reason, the Applicant respectfully submits that the Office Action has failed to establish a *prima facie* case of obviousness with respect to claim 36.

E. The Proposed Combination Does Not Render Claim 37 Unpatentable

Claim 37 recites, in part, "wherein cyclic redundancy check values for ciphered data are stored in the data update package." The Applicant respectfully submits that neither Selkirk, nor Nachenberg describes, teaches or suggests a "cyclic redundancy check." Thus, for at least this additional reason, the Applicant respectfully submits that the Office Action has failed to establish a *prima facie* case of obviousness with respect to claim 37.

F. The Proposed Combination Does Not Render Claim 40 Unpatentable

Claim 40 recites, in part, "a fault tolerant upgrade, the fault tolerant upgrade at least comprising: maintaining each original data block intact until the original data block

is overwritten by an encrypted updated data block; and maintaining a data update package intact throughout the fault tolerant upgrade." The Applicant respectfully submits that neither Selkirk, nor Nachenberg describes, teaches or suggests anything related to "fault tolerance." Thus, for at least this additional reason, the Applicant respectfully submits that the Office Action has failed to establish a *prima facie* case of obviousness with respect to claim 40.

III. Conclusion

For at least the reasons discussed above, the Applicant respectfully submits that the pending claims are allowable in all respects. Therefore, the Board is respectfully requested to reverse the rejections of pending claims 1-41.

Date: April 3, 2008

Respectfully submitted,

Hewlett-Packard Company
Intellectual Property Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400

/Kevin E. Borg/
Kevin E. Borg
Reg. No. 51,486

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1. An electronic device network for updating at least one of firmware and software in a plurality of electronic devices using at least one electronic device update, the network comprising:

at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine;

at least one update store storing a plurality of electronic device updates;

at least one update delivery server adapted to dispense the plurality of electronic device updates; and

wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted.

2. The network according to claim 1, wherein the at least one update delivery server comprises secure sockets layer support providing authentication and data encryption/decryption.

3. The network according to claim 1, wherein each of the plurality of electronic devices are adapted to retrieve secure encrypted updates from the at least one update delivery server to update the at least one of firmware and software resident in the plurality of electronic devices, and wherein at least a portion of the at least one of firmware and software resident in the electronic devices is encrypted.

4. The network according to claim 1, wherein each of the plurality of electronic devices comprise:

one of encrypting and decrypting components; and

a client for downloading updates.

5. The network according to claim 1, wherein each of the plurality of electronic devices comprise a security services component providing secure communication with the at least one update delivery server.

6. The network according to claim 1, wherein each of the plurality of electronic devices comprise an encrypted section, the encrypted section comprising at least one of an encrypted data section and an encrypted code section.

7. The network according to claim 1, wherein each of the plurality of electronic devices comprises at least one of a random access memory, a provisioned data section, an operating system, an update agent, and an update application loader, and wherein the provisioned data section comprises an update agent provisioning information section and a number assignment module.

8. The network according to claim 7, wherein the update agent is adapted to employ at least one of encrypting and decrypting components to update at least one of firmware and software resident in the electronic devices, and wherein at least a portion of the at least one of firmware and software is encrypted and stored in one of an encrypted data section and an encrypted code section.

9. The network according to claim 1, wherein the update generator is adapted to process an old memory image and a new memory image of the at least one of firmware and software in the electronic devices, and wherein at least a portion of the at least one of firmware and software is encrypted.

10. The network according to claim 1, wherein the update generator is adapted to decipher one of encrypted data segments and encrypted code in both an old memory image and a new memory image to generate an update for updating at least one of firmware and software in the electronic devices.

11. The network according to claim 1, wherein the update generator is adapted to employ deciphering techniques to extract one of enciphered code and enciphered data segments, process the one of enciphered code and enciphered data segments to generate an update comprising difference information, and encipher the one of code and data segments, and the difference information in at least one update.

12. The network according to claim 1, wherein the electronic devices comprise a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, a multimedia player, and a camera.

13. A method of updating encrypted information within a firmware image in electronic devices, the method comprising:

generating binary difference information using a first firmware image and a second firmware image, wherein one or both of the first and second firmware images are partially or entirely encrypted, and wherein generating comprises decrypting encrypted portions of the first and second firmware images;

creating an encrypted update for an electronic device using the binary differencing information; and

encrypting firmware images by applying at least one of stream symmetric enciphering and block symmetric enciphering.

14. The method according to claim 13, wherein stream symmetric enciphering is performed in a byte by byte manner, wherein update information is processed using a key stream to produce an encrypted update.

15. The method according to claim 14, wherein stream symmetric enciphering further comprises an i^{th} byte of the key stream operating on a byte of the update information produce an i^{th} cipher encrypted byte.

16. The method according to claim 15, wherein the i^{th} cipher encrypted byte is decrypted by the i^{th} byte of the key stream operating on the i^{th} cipher encrypted byte to reproduce an original i^{th} byte of update information.

17. The method according to claim 13, wherein block symmetric enciphering is performed upon blocks of data, wherein the blocks of data comprise a predetermined number of bytes, wherein a key block is applied to an update information block to

produce an encrypted block, and wherein block symmetric enciphering is performed by cipher block chaining.

18. The method according to claim 17, wherein the predetermined number of bytes in the blocks of data comprises 8-16 bytes.

19. The method according to claim 17, wherein block symmetric enciphering is enabled to accommodate variable block sizes, wherein block sizes are at least one of expanded and padded, wherein padding is one of added and removed to vary the block sizes during a ciphering process.

20. The method according to claim 13, wherein an enciphering algorithm and an enciphering key are stored in the electronic devices.

21. The method according to claim 13, wherein the electronic devices comprise a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, multimedia player, and a camera.

22. An electronic device employing one of encrypting and decrypting techniques to update firmware and software, the electronic device comprising:

random access memory; and

non-volatile memory, the non-volatile memory comprising:

an update agent;

a first in first out (FIFO) memory device;

a firmware;

a software application; and

an update, wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating, and wherein updating at least one of the firmware and the software application comprises decrypting the encrypted portion.

23. The electronic device according to claim 22, wherein the at least one of the firmware and the software application selected for updating in the electronic device are at least partially encrypted.

24. The electronic device according to claim 22, wherein the electronic device is adapted to retrieve secure encrypted updates from an update delivery server to update at least one of the firmware and the software application selected for updating resident in the electronic device.

25. The electronic device according to claim 22, wherein the electronic device comprises at least one of encrypting and decrypting components and a client for facilitating downloading updates.

26. The electronic device according to claim 22, wherein the electronic device comprises a security services component providing secure communication with an update delivery server.

27. The electronic device according to claim 22, wherein the electronic device comprises an encrypted section, the encrypted section comprising at least one of an encrypted data section and an encrypted code section.

28. The electronic device according to claim 22, wherein the electronic device further comprises at least one of a provisioned data section, an operating system, an update agent, and an update application loader, the provisioned data section comprising an update agent provisioning information section and a number assignment module.

29. The electronic device according to claim 28, wherein the update agent is adapted to employ at least one of encrypting and decrypting components to update at least one of firmware and software application resident in the electronic device, and wherein at least a portion of the at least one of firmware and software application is encrypted and stored in one of an encrypted data section and an encrypted code section.

30. The electronic device according to claim 21, wherein the electronic device comprises a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, multimedia player, and a camera.

31. A method of building a firmware upgrade for use in an electronic device incorporating encryption, the method comprising:

building a firmware image to be encrypted, the firmware image comprising a plurality of components; and

encrypting the components before assembling the components into an encrypted firmware image.

32. The method according to claim 31, further comprising:

generating binary difference information between firmware versions undergoing an upgrade; and

using an un-encrypted firmware image to generate the binary difference information, wherein as the upgrade is being applied to an encrypted firmware image, uncorrelated information is decrypted.

33. The method according to claim 31, further comprising creating a data update package, the data update package being based upon un-encrypted binary images.

34. The method according to claim 31, further comprising creating a data update package, the data update package being based upon encrypted binary images.

35. The method according to claim 31, further comprising at least one of:

managing encrypted information by performing a pre-check analysis;

managing encrypted information by performing a check-recovery analysis; and

managing encrypted information by performing a fault tolerant procedure.

36. The method according to claim 35, wherein during at least one of the pre-check analysis and the check recovery analysis, a cyclic redundancy check of a firmware image block is compared against an original image cyclic redundancy check stored in a data update package, wherein when ciphered data is present, the pre-check analysis is performed upon the block to be decrypted before the cyclic redundancy check is calculated.

37. The method according to claim 36, wherein cyclic redundancy check values for ciphered data are stored in the data update package.

38. The method according to claim 35, wherein during the fault tolerant procedure a ciphering algorithm is applied to facilitate recovery of data for the upgrade.

39. The method according to claim 31, further comprising:

decrypting an original data block and copying the decrypted data block to random access memory;

applying update information to the random access memory, the update information comprising at least one of an update code and an update data segment from a data update package;

updating the decrypted data block with the update information to form an updated decrypted data block;

encrypting the updated decrypted data block to form an encrypted updated data block;

sending the encrypted updated data block to a storage unit;

overwriting the original data block with the encrypted updated data block; and

processing every data block to be updated during an upgrade.

40. The method according to claim 39, further comprising a fault tolerant upgrade, the fault tolerant upgrade at least comprising:

maintaining each original data block intact until the original data block is overwritten by an encrypted updated data block; and

maintaining a data update package intact throughout the fault tolerant upgrade.

41. The method according to claim 31, wherein the electronic device comprises a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, multimedia player, and a camera.

EVIDENCE APPENDIX
(37 C.F.R. § 41.37(c)(1)(ix))

(1) United States Patent No. 6,230,316 ("Nachenberg"), entered into record by Examiner in June 20, 2007 Office Action.

(2) United States Application Publication No. 2003/0051160 ("Selkirk"), entered into record by Examiner in June 20, 2007 Office Action.

RELATED PROCEEDINGS APPENDIX

(37 C.F.R. § 41.37(c)(1)(x))

Not applicable.